Online Banking Fraud:
Extracting intelligence from Zeus configuration files

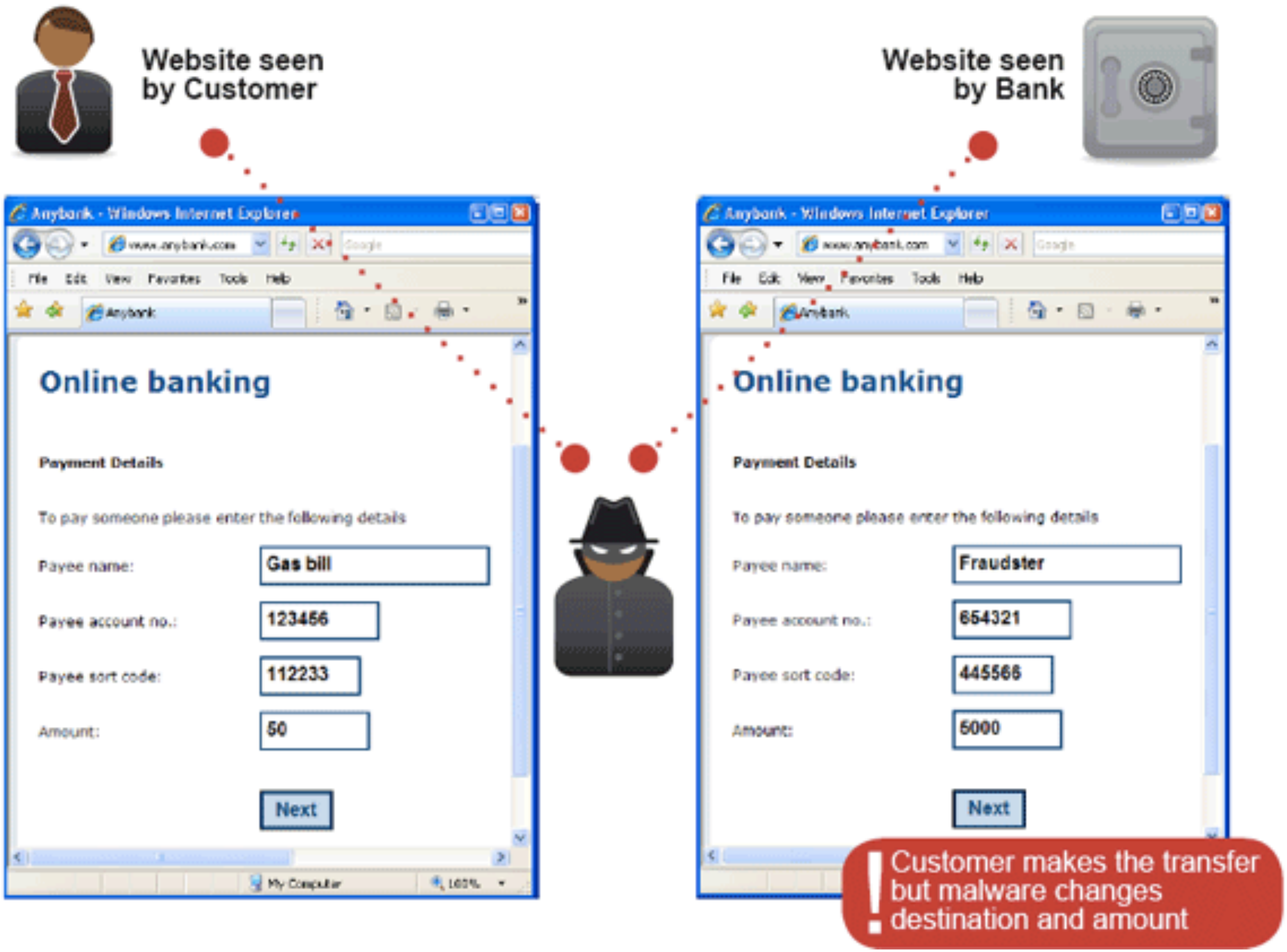
Samaneh Tajalizadehkhoob, Hadi Asghari, Carlos Gañán, Michel van Eeten

Delft University of Technology

The online banking fraud problem

- Fraud statistics for the Single European Payment area are around €800 million (European Central Bank, 2014)
- Different banks with different properties are targeted around the world
- No patterns have been found till now
- Little information is published about the targeted domains
- Even when the information exists, it is incomplete and under/over counted

Man in the Browser



Website seen by Customer

Online banking

Payment Details

To pay someone please enter the following details

Payee name:	Gas bill
Payee account no.:	123456
Payee sort code:	112233
Amount:	50

Next

Website seen by Bank

Online banking

Payment Details

To pay someone please enter the following details

Payee name:	Fraudster
Payee account no.:	654321
Payee sort code:	445566
Amount:	5000

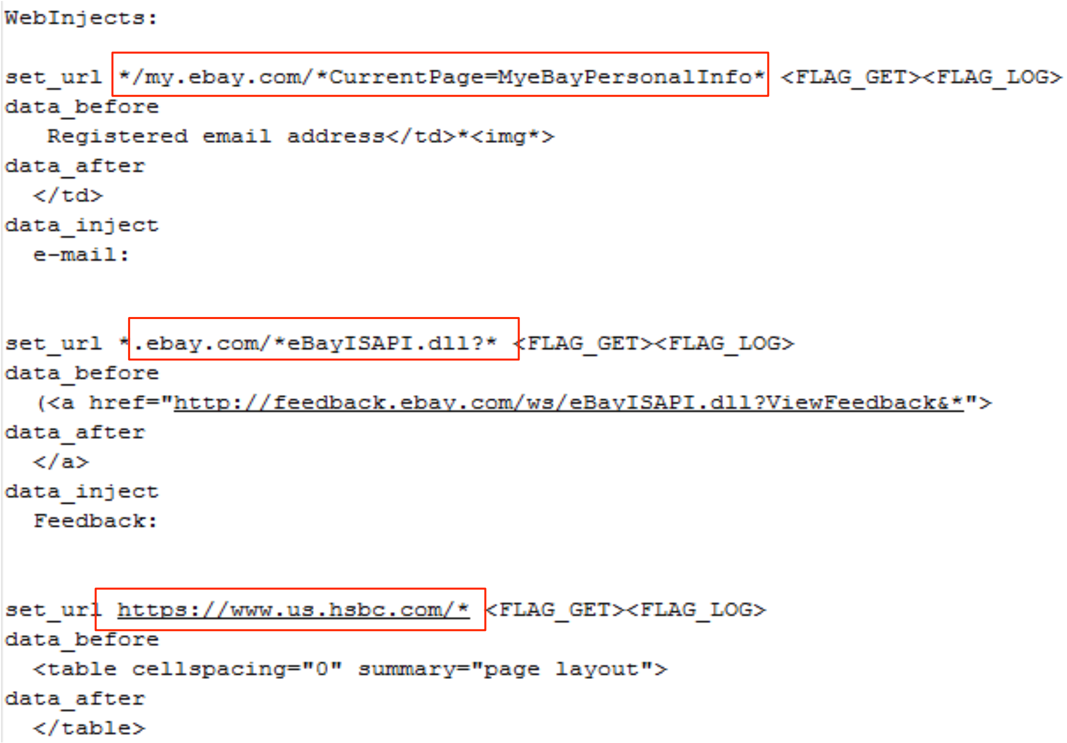
Next

! Customer makes the transfer but malware changes destination and amount

Methodology

Fox-IT provided access to 11,000 records of Zeus financial malware configuration files from 2009 to 2013Q1. The file contains instructions on:

- which target to attack
- what user data to gather
- how to do so



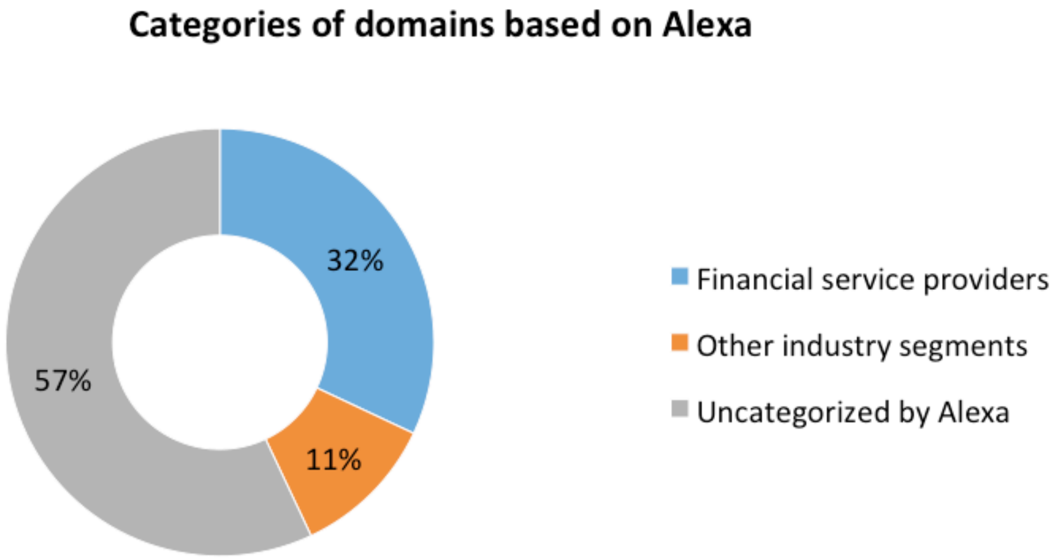
```
WebInjects:

set_url */my.ebay.com/*CurrentPage=MyeBayPersonalInfo* <FLAG_GET><FLAG_LOG>
data_before
   Registered email address</td>*<img*>
data_after
  </td>
data_inject
  e-mail:


set_url *.ebay.com/*eBayISAPI.dll?* <FLAG_GET><FLAG_LOG>
data_before
  (<a href="http://feedback.ebay.com/ws/eBayISAPI.dll?ViewFeedback&*">
data_after
  </a>
data_inject
  Feedback:


set_url https://www.us.hsbc.com/* <FLAG_GET><FLAG_LOG>
data_before
  <table cellspacing="0" summary="page layout">
data_after
  </table>
```

Questions

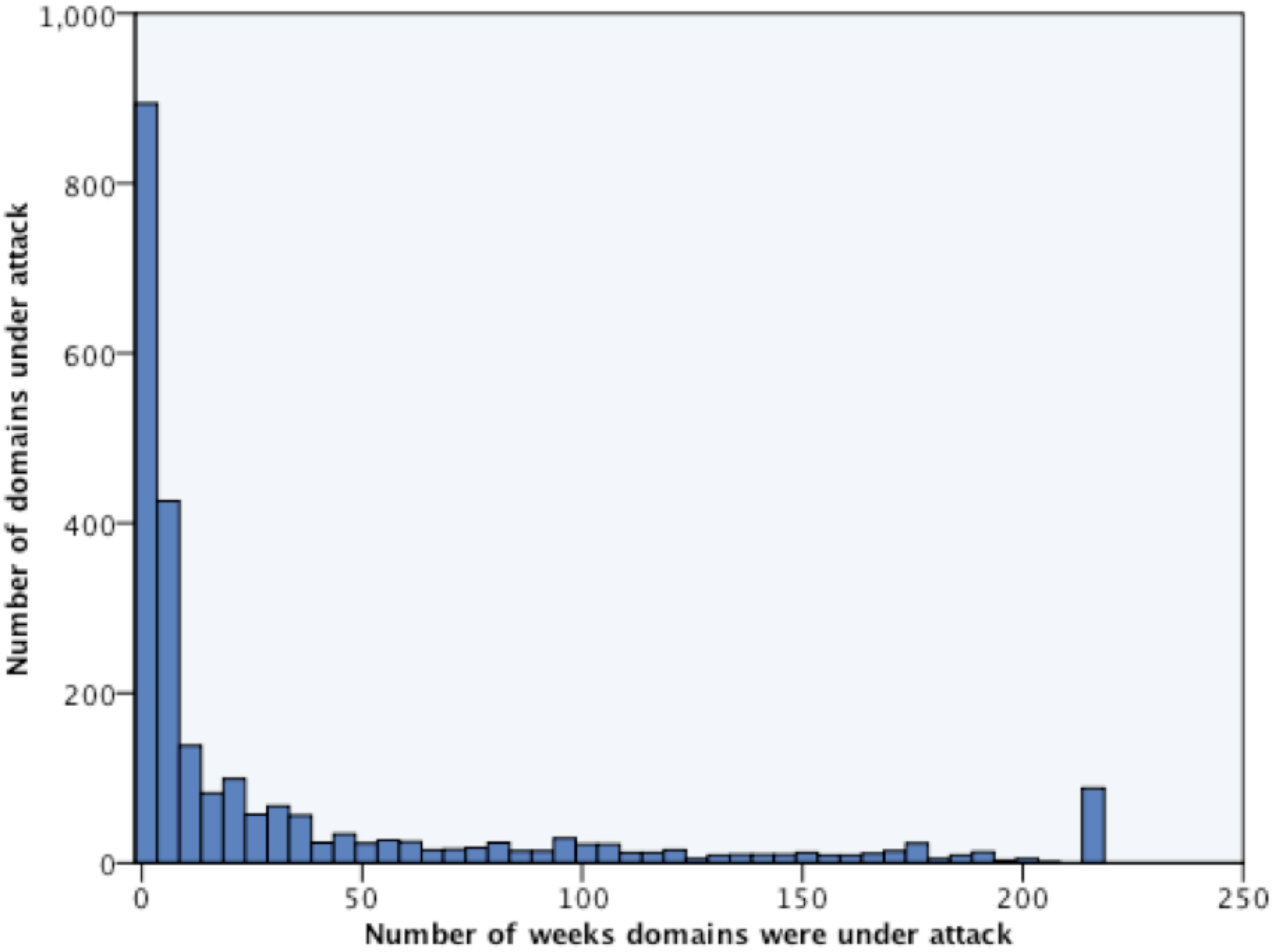
- What type of domains are targeted via ZeuS?
- Are some financial services targeted more often than other?
- Why?
- How are new targets identified over time?
- What is the impact on attack volume of attack code becoming more easily availabe over time?
- How quickly does attack code (web injects) develop over time?

Findings - targeted domains

- Over 4 years, we saw 2,412 unique domains targeted – via14,870 unique URLs
- Located in 92 countries
- From 2,131 unique botnets (based on different encrypted command and control channels)
- Over 74% of the targets are financial service providers

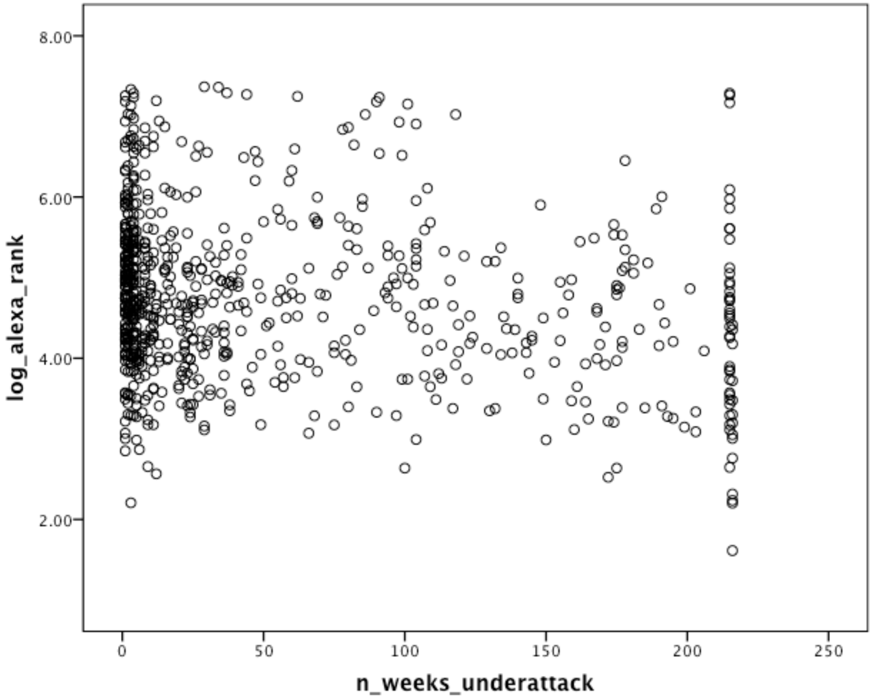


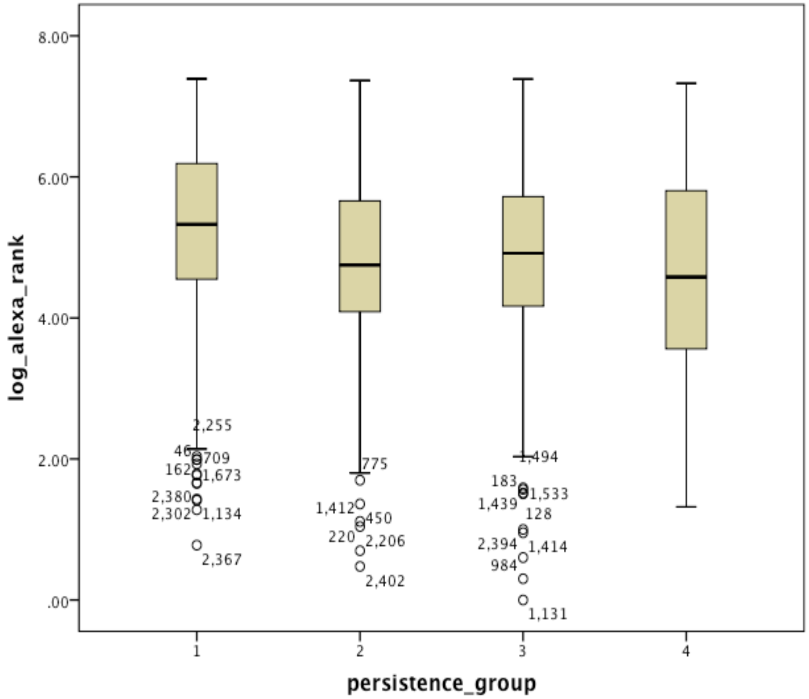
Findings - attack persistency



Is target popularity related to its size?

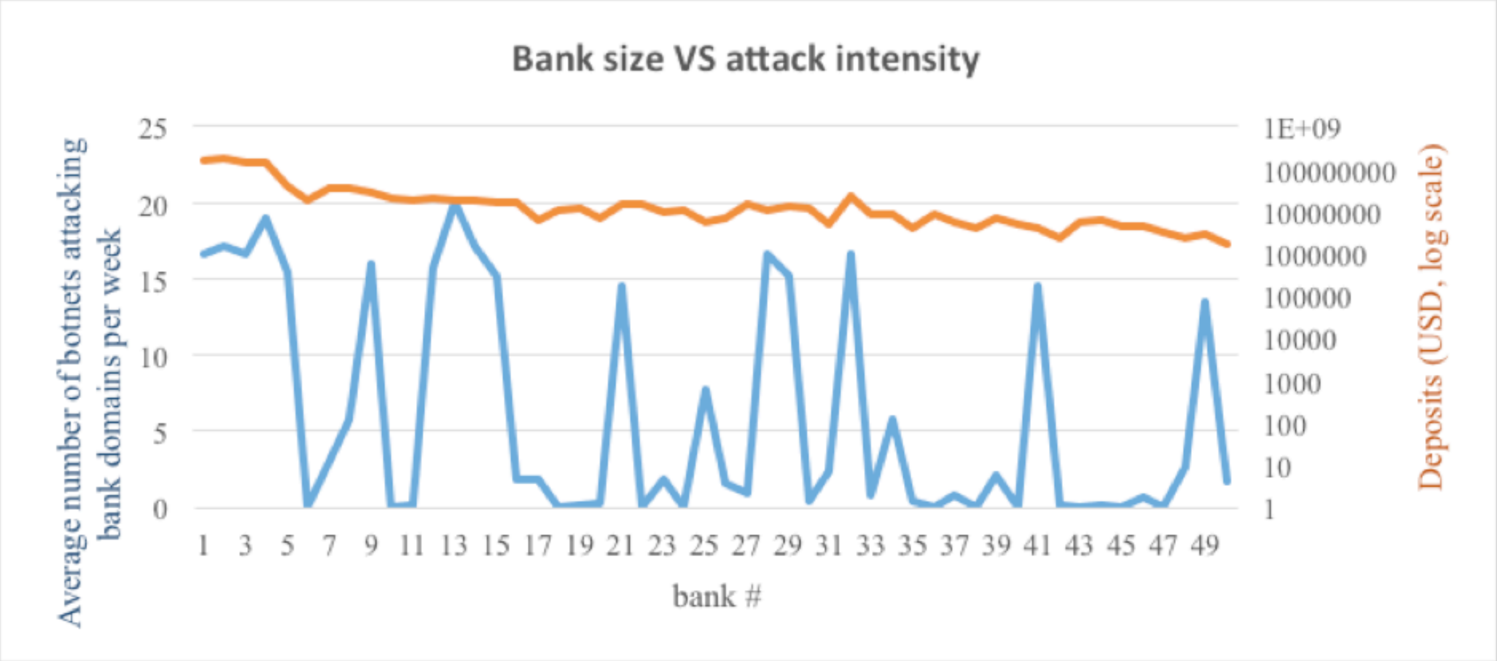
- There is a minor, but significant relationship between the size of a domain (measured by Alexa ranking) and the persistency of attacks



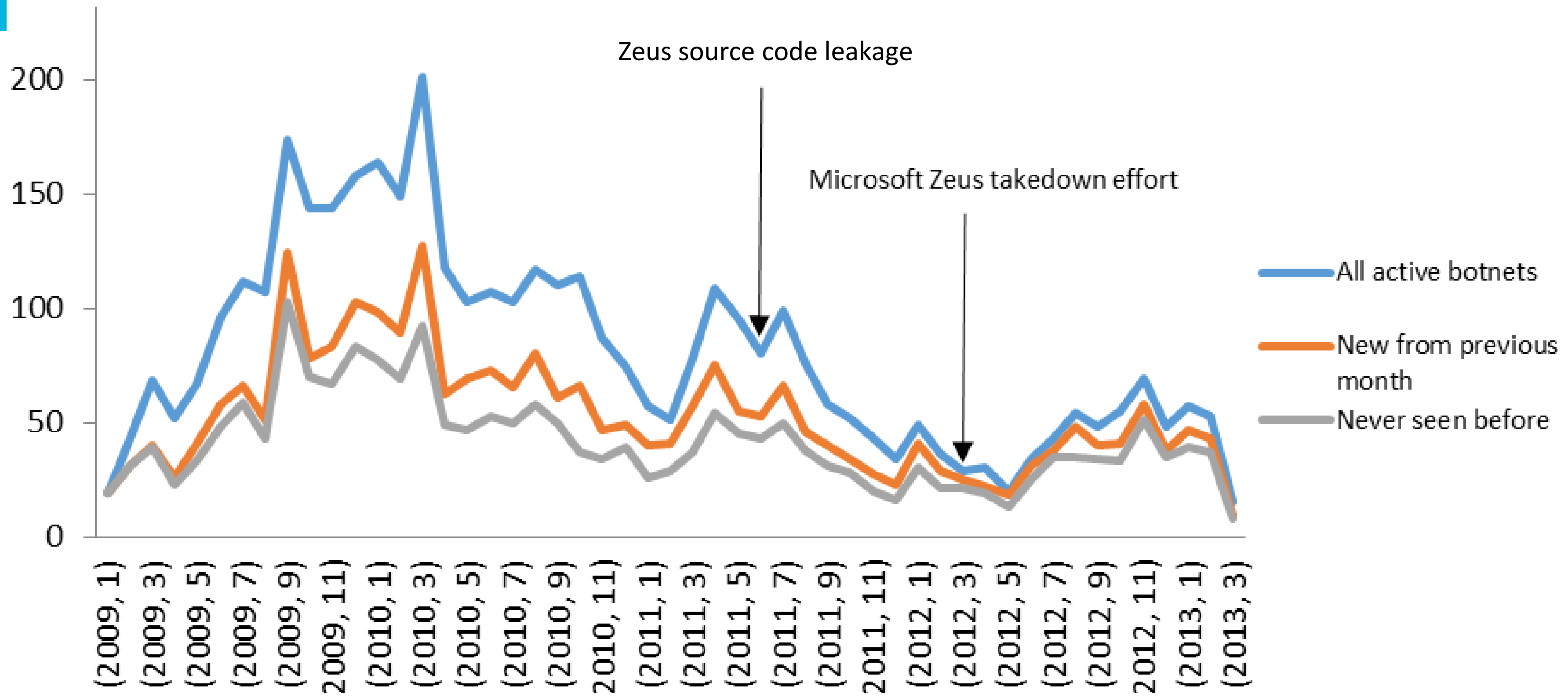


Is target popularity related to its size?

- United States: out of around 6,500 active financial institutions, only 175 have been targeted
- Almost all of the larger banks (48 of the top 50) are attacked
- Size acts as a threshold for being attacked; it does not predict attack intensity

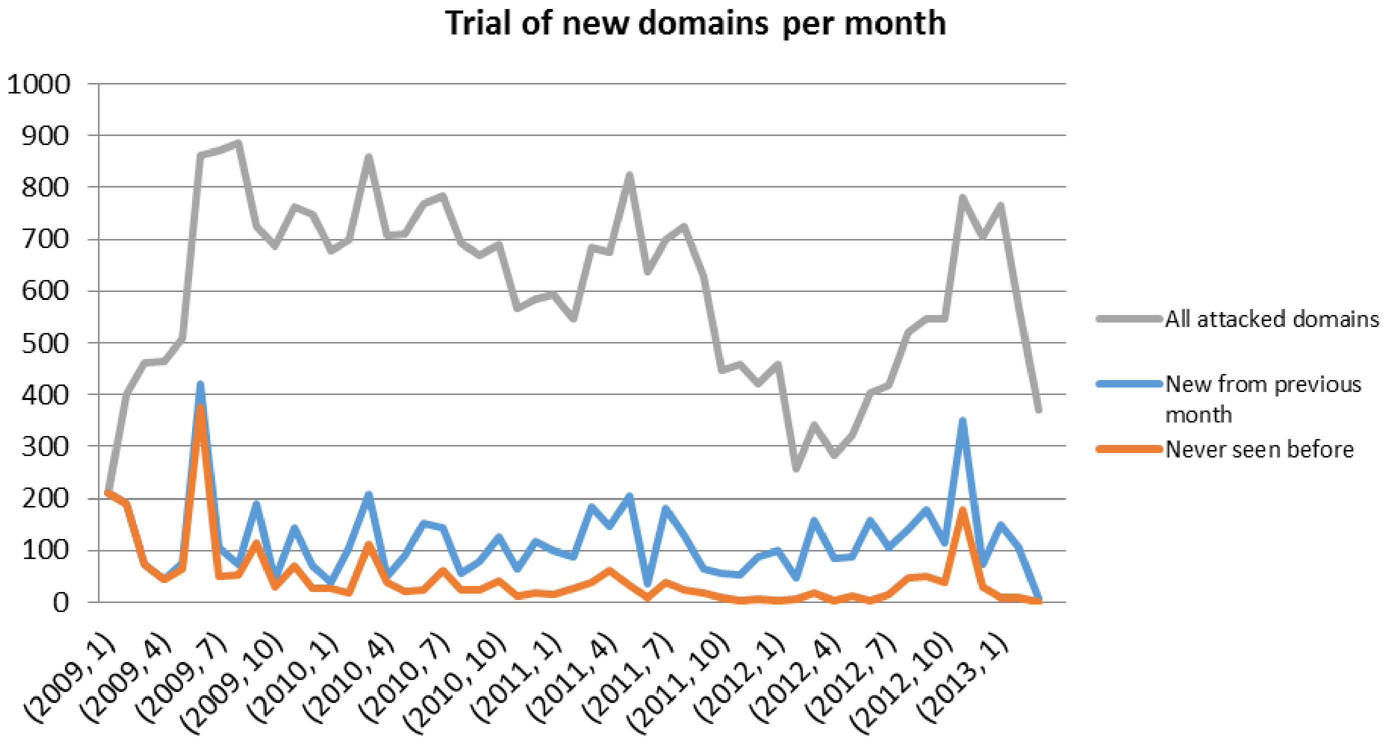


Number of active botnets



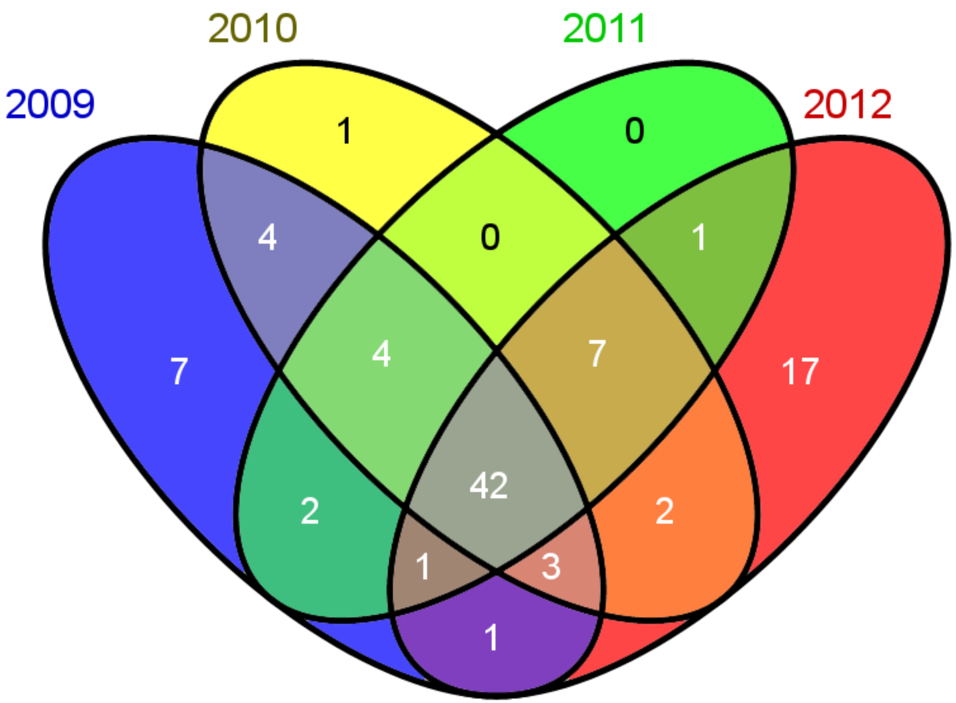
Trial of new targets

- On average, 601 domains each month become targets of Zeus attacks
- Out of these on average, 112 of these are new domains each month
- There is a stable ceiling in the number of attacked domains, as well as in the trial and error or new targets



Trial of new targets

- Seeking new targets across a larger area
- In 2012, 17 new countries were targeted, but 18 countries from the previous years were no longer being attacked



Summary

- Not every Financial Service Provider is equally popular among criminals
- Size is a threshold for getting attacked, but does not predict the intensity
- Attack persistence varies widely. Half the domains are targeted briefly, mostly likely in search of new targets
- A ceiling exists in the overall number of domains simultaneously attacked, even after the ZeuS code leak

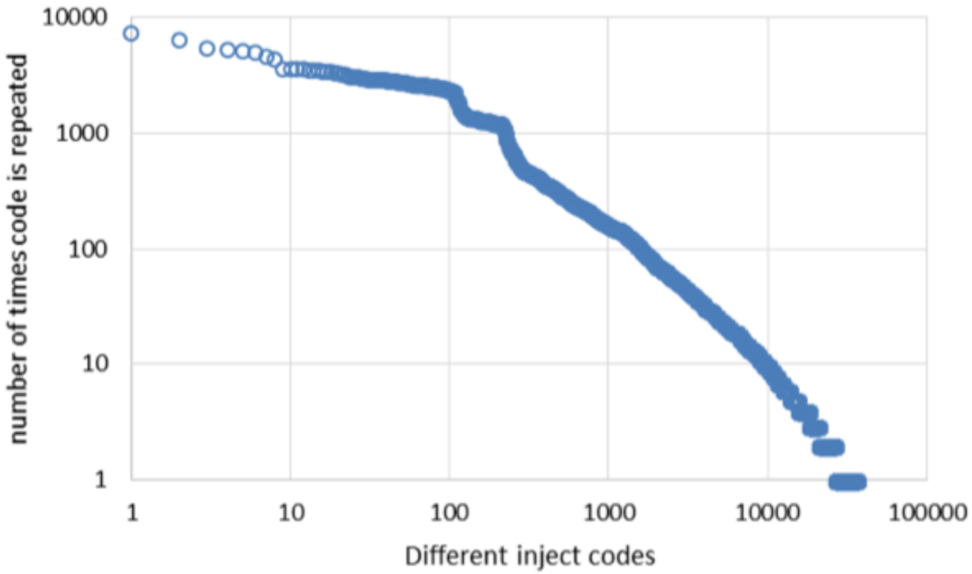
Summary

- Attacks to the same URL are more than 90% similar, no matter the length of the inject; this suggests code sharing, stealing or selling (inject-code-as-a-service) among criminals;
- Attacks (and defense!) is less dynamic than often presumed
- The underground market for bots and malware may have lower economic entry barriers for criminals and reduced costs in the value chain of attacks, but it has not increased attack volume (number of botnets) or the number of targets
- Attack ceiling suggests other bottlenecks in the criminal value chain, such as in cash out operations and mule recruitment
- Defense should focus on these bottlenecks, not on reducing abundant attacker resources (i.e., bots, malware and injects)

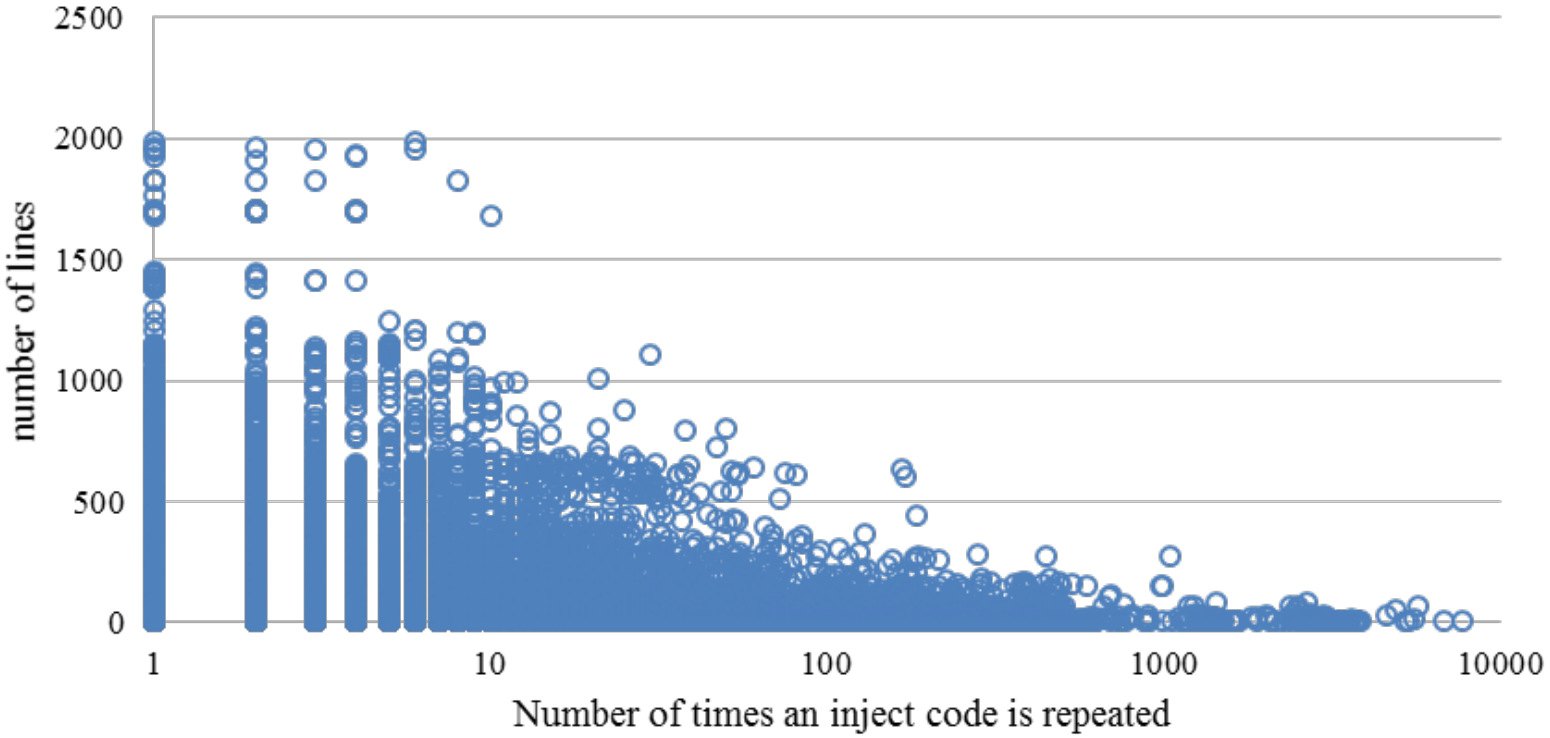
Question?

Inject code development over time

- The data contains 1.1m target URLs with ‘inject’ codes.
- On average, each inject code is repeated 27 times; 43% repeated over 1,000 times, and just 1% appears once!
- Substantial amount of inject code sees no or very little development over time
- High level of code re-use suggests sharing, stealing or selling code across attackers



Inject Code Size vs. Repetition



Next steps

- Map security properties of attacked services (e.g., authentication mechanism)
- Study interaction among attack and defense (e.g., deterrence, waterbed effect?)
- Statistically model factors that determine fraud levels in countries
- Identify most cost-effective countermeasures